CHAPTER 3

The Public-Private Partnership in Critical Infrastructure Protection

Introduction

Mr. Frank Ciluffo

Director, Homeland Security Policy Institute,
George Washington University

When you translate some business concepts into factors in security, you need to understand the capabilities of those who will be responsible for implementing and executing any proposed solutions. The solution for CIP clearly rests with the private sector, which owns the bulk of our critical infrastructure. The implementation of self-initiated security standards by the private sector is the desired solution. However, market forces can only drive security to a certain level; we need to identify new means to elevate security to the next level. These means should include incentives for private sector entities to strive to achieve that next level of security standards. One incentive is a degree of indemnification for those industries that seek to do the right thing and meet or exceed their standards for security.

The public-private partnership is the critical element for CIP. And that partnership should include—beyond the owners and operators—those who insure the infrastructure; and the insurance industry should be involved in any effort to develop self-initiated security standards and best practices, as well as the methodologies for evaluating their implementation. This session will explore the Public-Private Partnership in Critical Infrastructure Protection. It begins with Ms. Marilyn Ware, CEO Emeritus of the American Water Company, who will discuss the "Challenges of the Partnership: Pulling together the Public and Private

Sectors." She will be followed by Mr. Al Martinez-Fonts, who is the Department of Homeland Security's primary point of contact for the private sector; he will give us a look at the "Sticks and Carrots: Incentives and Regulations for the Private Sector." Finally, Mr. Harrison Oellrich of Guy Carpenter and Company will speak about "Strategies, Policies, and the Private Sector" from the standpoint of the re-insurance industry.

Challenges of the Partnership: Pulling Together the Public and Private Sectors

Marilyn Ware

Chairman, Ware Family Offices

This symposium, "In Support of the Common Defense: Examining Critical Infrastructure Protection in the Public and Private Sectors" organized by the Center for Strategic Leadership is both relevant and timely. I have been asked to provide observations on the challenges we face as a nation as we attempt to bring the public and private sectors together in the interests of national security. My observations are based on my own experiences in the water business as well as my recent participation with others from a range of industries, all of whom have been tasked with improving the collaboration of public and private sectors in matters of national security.

Since the tragic events of September 11, 2001, the nation has been evolving along a homeland security continuum, beginning with an evaluation process, wherein we paused to take account of a new security paradigm. The creation of the Department of Homeland Security (DHS) and its initial activities to develop a National Infrastructure Protection Plan (NIPP) just this year [2004] marked the second phase in this evolution—adaptation. We are about to embark on the third and most difficult stage—transition.

Change of this importance and at this scale will not happen quickly, however. I will argue in this paper that key to the adaptation phase, in which we find ourselves today, is the fundamental realization that no single government entity or any single sector could possibly find all the right answers working alone. Instead, we have turned to a public-private partnership model to explore the issues and find solutions. I will argue further that transition will be characterized by implementation and refinement of this partnership model. This transition will be far more effective if the public and private sectors can address their differences

in risk aversion, in performance-based rewards, and in our divergent approaches to competition.

Introduction

One of the explicit goals of DHS is to improve the collaboration between government agencies and the private sector in matters of national security. To this end, the President established the National Infrastructure Advisory Council (NIAC) by Executive Order 13231 of October 16, 2001, as amended by Executive Order 13286 of February 28, 2003. The NIAC is charged with enhancing the partnership of public and private sectors in protecting the information systems that underpin all CIP issues. NIAC members are appointed by the President and selected from the private sector, academia, and State and local government. Through the Secretary for Homeland Security, NIAC provides the President with advice on the security of information systems within each of the seventeen critical infrastructure sectors named in HSPD-7, dated December 2003.[1] Among others, these sectors include:

- Banking and finance
- Transportation
- Energy
- Manufacturing
- Water
- Public Health
- Information and Telecommunications
- Emergency Government Services

This paper first reviews the work of the NIAC to date, drawing examples of certain aspects of public-private partnerships that have emerged in these sectors. It then addresses the evolution of thinking within the security community more generally about why these partnerships are so important to the security of the nation and where from a policy perspective, we need to head in the next phase of their development. Finally, it concludes with a few key principles that need

[1] HSPD-7 named 13 critical infrastructure sectors and 4 additional sectors as "key resources." For convenience, this paper refers to all 17 sectors as critical infrastructure.

to guide our partnership efforts to ensure that we achieve our national security goals in the most effective and efficient manner, as we adapt and transition to the new security paradigm.

Why Are Partnerships Important?

Homeland security is much like defense from many important perspectives. Both are most efficiently organized and managed centrally. Both require Federal government leadership since they are delivered at scales beyond the capacity of any single non-Federal government or any industry or sector. Both deliver broad benefits to many individuals and companies simultaneously, but are difficult to isolate and deliver only to a single recipient. Both rely on sophisticated and specialized networks of information and infrastructure.

But homeland security is unlike defense in other important ways. Defense protects principles of society like freedom and democracy and is deployed spatially across vast distances such as national borders, which are not owned by any single enterprise or government. Homeland security, on the other hand, protects private property, community well-being, the personal safety of 294 million Americans, and the domestic economy more generally. So while it is entirely reasonable for the American public to ask the Armed Forces to organize and deliver defense services on our behalf, our homeland is comprised of hundreds of millions of parcels of land, public buildings, public works infrastructure, and private businesses in all fifty states. Even if the public were willing to ask the DHS to deliver security services on our behalf, it simply would not be possible. Instead, we ask the Federal government, working through DHS, to help organize the homeland security effort (since it's scale and importance are so much like defense), but engage other government entities, academia, and the private sector to coordinate delivery of homeland security services. Partnerships among government entities and between public and private sector entities are the most crucial component in achieving this engagement.

Command and control approaches to CIP cannot be expected to work. Critical infrastructure sectors like finance and banking, energy, water, telecommunications, or transportation are composed of networks of interrelated physical, cyber, and human assets. These assets are designed and operated to deliver services to households and businesses

across America—indeed, across the world in many cases—as seamlessly as possible. When interrupted, either unintentionally as a result of a severe weather event or intentionally through an act of terrorism, not only can these networks fail, but failure in one location can cascade to many other locations across the sector network. Of course, failure in one infrastructure sector can result in failure in other linked infrastructures

Consider, for example, the aftermath of the attacks in New York City on September 11, 2001. Paul Bennett, who runs the security department of the New York City Municipal Water Department, had an emergency plan in place, a plan on a scale that he believed adequate based on history. But suddenly, on September 11, he found himself thrust into a situation where he had to manage a crisis of a proportion that he had never imagined, without critical linkages to other infrastructure or response assets. On top of that, he found himself robbed of the product that others in the City needed the most during the recovery effort. The water pipes that led into his sector were damaged. He could not find fire hydrants. He could not find water mains. They were buried beneath tons of debris. Roads were blocked so his trucks were useless. Phones were not operational, so his staff could not coordinate their efforts or those of other City workers. All the emergency response resources in the City and the region were consumed. His response plan was totally inadequate because the linkages to other infrastructures and human resources had been severed. Despite all this, however, the NYC Water Department began to re-establish both their water and wastewater networks, which were essential to wash down firemen and fire trucks, keep debris stable, and accommodate wastewater of unknown quality flowing into the City's treatment plants.

Of course this only one and perhaps an extreme example. But more generally, given this high degree of interconnectedness both within and across infrastructure sectors, the rationale for partnerships is compelling. Each critical infrastructure must develop its own security strategy that deals consistently with readiness, response, and recovery based on assessments of threats to the sector and an understanding of vulnerabilities specific to its own unique assets. But because of their interconnectedness, sectoral strategies and protection measures also must be linked to the systems developed to protect other infrastructure sectors. Creating this "system

of systems" can be accomplished only through information sharing and partnerships not only within sectors, but across sectors.

What Kinds of Partnerships Deliver Effective Homeland Security Services?

As the previous section argued, neither a single level of government nor the private sector alone can or should be responsible for the security of our homeland. America's seventeen critical infrastructure sectors are too diverse, too complex, and too interdependent. Instead, each level of government and the private sector has a unique role to play directing its own activities and managing or participating in a series of partnerships to create a "system of systems" approach to homeland security.

The NIAC has developed a framework to evaluate whether and the extent to which government intervention—one form of which are partnerships among governments or between governments and the private sector—makes sense, both across and within sectors. The NIAC framework observed the following:

1. A deep understanding of sector dynamics is needed for effective intervention
2. Organizations are responding through competition and cooperation, to address threats
3. Government action may be required in some sectors
4. A common framework may be used to discuss the role of market intervention
5. Identified best practices should be considered when intervention is planned

A deep understanding of sector dynamics. The extent to which government can be effective in working with private owner/operators is entirely dependent on how well government interventions—partnerships included—account for specific conditions that characterize each sector and the significant differences from one sector to the next. About 85 percent of all critical infrastructure in the U.S. is owned and operated by private companies. In some sectors, such as telecommunications or manufacturing, all infrastructure is privately owned. The extent to which critical infrastructure sectors operate under purely market conditions differs widely, with some sectors like manufacturing perhaps

operating purely in response to such conditions. Some sectors such as telecommunications are regulated at the Federal level; others like water or energy are regulated at the State level; and still others like banking and finance are regulated through international accords. Whereas a single terrorist event lodged against the payment system of the Federal Reserve Bank, for example, could have a significant effect in the national economy, for other sectors such as public health, it would take widespread, coordinated attacks against multiple infrastructure locations to have a similar national impact.

Under these conditions, partnerships with infrastructure owner/operators are critical first, to evaluate whether interventions are needed at all, and if they are, how they might be optimally structured. Higher security standards and more government attention, for example, may be appropriate for sectors with high degrees of interconnectivity like electricity distribution or sectors like finance, for which failures could result in nationally significant effects. The nation's transportation sector, in contrast, is characterized by a very high degree of redundancy, so failure in one location is unlikely to have widespread effects. A somewhat reduced security standard, or no national standard at all, may be appropriate in these circumstances.

Organizations are responding to threats through cooperation and coordination. In many sectors including some of the critical infrastructure sectors that NIAC examined, market forces are the single strongest driver of security behavior. Where this is the case, companies recognize how their critical assets can be damaged by malicious intent, and respond effectively to the threat. In some sectors, sector-led initiatives and regulations effectively augment market forces as drivers of security. Industry groups such as the North American Electric Reliability Council (NERC) and the American Chemistry Council (ACC) have published mandatory security guidelines for their sectors. However, the strength of the enforcement mechanisms can vary. The ACC's guidelines are self-enforced, though physical site security enhancements currently are independently audited, and ultimately all aspects will be. The NERC can notify the Federal Energy Regulatory Commission (FERC) of electric companies not in compliance, bringing unwanted regulatory scrutiny.

Where sectors are effectively self-regulated on security matters, the government role in partnerships is modest, typically focusing on information sharing and/or performance measurement

Government actions may be required in some sectors. In some sectors, there are few incentives to enhance security and indeed, there may be disincentives. In the water sector, for example, there are 161,000 public water systems that serve twenty-five or more people. Of these, some 160,000 systems serve fewer than 50,000 people each, but 134 million people in total. Many of these smaller systems believe that terrorist attacks could never happen to them and consequently take few if any protective measures. While that may be appropriate based on past experiences, a significant portion of the U.S. population may be under-protected going forward. A coordinated, simultaneous attack against a dozen water systems would not cripple the American economy to be sure, but it would have potentially serious effects on the sense of well being of tens of millions of people that live in these smaller, under-protected communities. Because it's ingested, contamination of drinking water at any scale will have deep psychological impacts on people all across the country.

Under these circumstances, government participation in a nationwide partnership to strengthen the security consciousness of municipal and private water systems may well be appropriate. In general, government actions distorting the market least—those that add transparency and improve the operations of market forces—generally are best.

A common framework to shape the role of government action. Here, the NIAC suggests application of a series of screening criteria to refine circumstances in which government action may be needed in security partnership with infrastructure owner/operators:

- Where network interdependencies suggest potentially widespread effects from a terrorist attack
- Where security concerns do not drive customers to switch service providers (commodity purchasing of chemicals, for example) or where switching is not possible (natural monopolies, for example)

- Where voluntary sector activity to reduce security risks from terrorist activities is not occurring
- Where peer pressure within a sector fails to result in voluntary security measures
- Where attacks occur infrequently (or not at all, as yet), thus undermining the urgency of threats
- Where a terrorist attack could cause catastrophic injury or major economic damage
- Where industry profitability is too low to invest in security or where financial flexibility to invest and recover costs through pricing mechanisms is limited
- Where professional expertise is insufficient to execute an effective security assessment and plan

The NIAC was clear, however, that even in circumstances that meet some or all of the above criteria, the form of government participation up to and including regulation, must be carefully planned in partnership with sector participants to avoid excessive disruption in the sector, add value to the sector, and phase in over time.

Best practices should be considered when interventions are planned. While it seems obvious, it is nonetheless worth restating that government intervention of any kind must be developed in partnership with the sector in question. Plans that are developed through public-private partnership will build on existing best practices, recognize sector-specific needs and have a higher degree of buy-in from sector participants. Strong private-public collaboration, for example, was used in drafting the FFIEC (Federal Financial Institution Examination Council) regulatory handbook, which is broadly recognized by the banking industry for its value. Given the scarcity of resources for enforcement, regulations that lack sector buy-in are generally less effective. The EPA's Underground Storage Tank (UST) program regulates leak detection and prevention in tanks containing petroleum or hazardous substances. However, more than 60 percent of states cannot inspect facilities in-line with the EPA's recommended once-every-three-years guideline due to under-staffing.

The NIAC offered several other guidelines for the government role in security partnerships:

- Mandates should address outcomes as opposed to specific actions to enable sector participants the greatest flexibility to adapt efficiently and recognize potential voluntary efforts of early movers
- The efforts of all levels of government should be carefully coordinated to avoid duplication of effort and potentially conflicting or confusing requirements
- Examine existing sector rules for their effects on security to ensure that partnerships also eliminate barriers to good security practices
- Build in regular review and flexibility of roles and rules to ensure that partnerships can change as the sector evolves or conditions themselves change
- Funding may be needed to back government mandates, especially where assets are owned by the public sector, or where barriers exist to recovery of costs in the private sector
- Implementation should be phased in to allow owner/operators of critical infrastructure sufficient time to adapt in stages

These observations have clear implications for the types of interventions or partnerships that are needed among governments and between government and the private sector to deliver effective and efficient homeland security.

Federal Partnerships. At the Federal level, partnerships must focus on issues of *governance*. Among the most important are:

- Setting homeland security strategy, including where appropriate, nationally applicable standards
- Justifying and distributing homeland security resources
- Removing obstacles that prevent effective and efficient delivery of homeland security actions at all levels of government and the private sector
- Driving consistency in the levels of homeland security across sectors

- Ensuring consistent response of enterprises within a sector to national risk reduction strategies and threshold levels of protection
- Measuring performance of our national homeland security initiatives
- Using performance measures to drive continuous risk reduction equitably across the economy

Partnerships among the Federal agencies with homeland security responsibilities are perhaps the most obvious, with creation of the DHS in 2002 one key step forward.

In December 2003, the President issued HSPD-7 to guide activities of the CIP effort. It directs Federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure (CI), defined to include thirteen named CI sectors plus four additional key resource (KR) sectors. It also requires that DHS take a leadership role with other Federal agencies and departments in working with State, local, and tribal governments and the private sector to carry out these responsibilities. HSPD-7 also identified the NIPP as the mechanism for consolidating and documenting security efforts to protect America's CI/KR.

In its "Base Plan," DHS has established national security goals, a framework for consolidating the security efforts of each of the seventeen CI/KR sectors, and a series of actions to be taken at all levels of government and in the private sector to implement security programs across the CI/KR sectors. Each of the seventeen sectors also produced a sector-specific plan, following the general framework in the base plan. These plans will form the basis for our nation's security initiative going forward, with specific actions named to protect cyber, physical, and human resources at all levels of government and the private sector now and well into the future. Figure 1, from DHS, captures the essence of this grand partnership among governments and the private sector to coordinate at the highest level, CIP via perhaps the largest and most ambitious partnership managed at the Federal level.

But equally important are the partnerships between Federal security agencies and other levels of government and private owner/operators of critical infrastructure. One series of partnerships that fit this

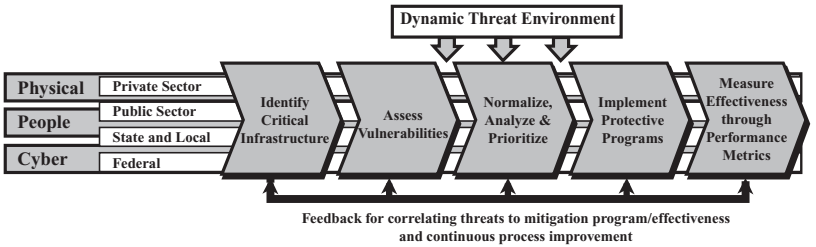

Figure 1: The Public-Private partnership for Critical Infrastructure Protection

category are the eleven private-sector Information Sharing and Analysis Centers (ISACs) that serve their corresponding sectors. ISACs serve as the principle mechanism to share strategic, operational, and tactical information among sector entities and between the sector and DHS. Strategic information, which is predominantly led by the intelligence community and/or Federal and State law enforcement, is focused on threats and their potential harm to critical infrastructure. Sector entities direct much of the sharing of operational information on such matters as how the sector supports systems to provide security services and risk reduction to large numbers of people and ultimately to the defense of the homeland. Tactical information sharing is centered on early warning of and first response (emergency services, law enforcement, etc) to terrorist incidents.

To date, participation in and performance of these ISACs is uneven, although efforts are underway within DHS's Information Coordination Division and the individual ISACs to enhance the information sharing process. Many ISACs are now communicating with their lead government agencies and DHS to cover a wide range of information-sharing issues affecting individual sectors, and their operations. Much of this increased communication is due to the support provided by the lead agencies. Increased communication has been instrumental in helping define common areas of interest. The NIAC has observed the following with respect to improving the effectiveness of ISACs:

> Scaling ISAC membership to include most infrastructure owners and operators in each sector would provide a broader base for information collection about threats for ISAC analysis and warnings. It would also provide a broad base to transmit warnings, countermeasures and other solutions. Federal funding

> support may enable ISACs to include a greater percentage of their sectors than they are currently capable of doing. Successful research toward real-time, cross-sector event correlation will add significant value to threat warning, trending and analysis. Enhancing trust models will encourage cross-sector and public-private information sharing, thereby enabling the Federal government to make timely decisions regarding possible attacks on the United States.

Many now believe that Sector Coordinating Councils (discussed below), as mandated by HSPD-7, are the future of sector coordination and communication activities and that DHS's Homeland Security Information Network (HSIN)—a self-contained, one-stop shop for threat and other information for all sectors—should displace ISACs all together. The HSIN is a national communication platform that allows the flow of real-time information among DHS, State, local, and private sector partners at the "sensitive but unclassified" level. The platform provides for features such as alerts, warnings, and advisories dissemination, real-time planning and problem solving, and information storage, search, and retrieval. Approximately 1,000 law enforcement entities, representing the Joint Regional Information Exchange System (JRIES) community of users, have access to the system.

State Partnerships. At the State level, partnerships need to be focused on issues of *accountability*. In our federalist form of government, states already have many of these responsibilities, including for example, regulating prices and quality of certain services delivered through efficient natural monopolies, assessing needs of enterprises within their boundaries, allocating resources equitably across jurisdictions, and aggregating social services for delivery across the state. In the context of homeland security, partnerships at the State level must deliver these same types of functions:

- Regulatory mechanisms that recognize and reward owner/operators of critical infrastructure that take security actions consistent with national priorities
- As an intermediary for Federal policy setters and performance managers, assurance that local jurisdictions and owner/operators of private critical infrastructure are managing risk consistently

- Allocation and distribution of resources where they are otherwise appropriate
- Creation and delivery of statewide response and recovery actions

One of the key interactions between State agencies and critical infrastructure owner/operators is in the area of regulation of both quality and prices of utility services such as energy, telecommunications, or water. Of course, these three sectors also are CI sectors named in HSPD-7. Consequently, a large opportunity exists to deal with regulatory issues through partnership initiatives managed at the State level. Currently, State regulatory agencies have established formal rate review and approval processes that govern whether and the extent to which consumers must pay for invested capital and operating costs of these utility services. On the one hand, these processes protect the public interest, but on the other hand, they are complicated, time consuming, and expensive. State regulators could begin working immediately with applicable CI sector coordinators to design new rate review and approval processes that reduce the burden on public and private entities seeking to recover security investments through rate adjustments. In particular, where such investments are consistent with sector directives and follow standardized, consistently applied methods, rate reviews should be perfunctory.

Another area where State-managed partnerships can be significantly strengthened is in the area of training and technical assistance. Opportunities exist in both the public health sector in the formation and readiness of deployable medical assets and the emergency government services sectors in creation of mobile emergency response teams.

Local Partnerships. At the local level, partnerships must focus on responsibility for *implementation*. Local governments and owner/operators of private CI are principally responsible for assessing their own vulnerabilities to terrorist attacks, planning and implementing practical risk reduction measures, preparing themselves to respond to terrorist events should they occur, and planning recovery from such attacks. All of these locally implemented measures are designed to prevent attacks where that is possible and otherwise limit their consequences should they occur.

For many types of CI, these tasks require a significant degree of cooperation with others within the sector as well as State and local agencies that stand ready to assist them. Formal partnerships to activate such cooperation can be particularly effective at the local level, where resources are generally limited, large risks are difficult to bear, and access to basic information like threat assessments is limited.

The greatest risks to the nation are at this level, since this is where failures to CI systems have occurred in the past and are most likely to occur in the future. Yet, paradoxically, the nation has under-invested in the development of effective partnerships that engage the local level.

Just now emerging, are a series of key partnerships in the form of Sector Coordinating Councils (SSCs), as contemplated in HSPD-7. These Councils are self-organized and sector-led coordination mechanisms that include comprehensive representation from both asset owners and operators and trade associations. They identify, prioritize, and coordinate sector programs to protect CI; and facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and security best practices. Once formed in cooperation with DHS, Councils, preferably through an owner/operator spokesperson, represent the principal mechanism for local input into Federal policy as well as the principal point of entry of government into sector-level infrastructure protection activities and issues. The SSC serves as an honest broker to facilitate inclusive organization and coordination of a sector's policy development, infrastructure protection planning, and plan implementation activities. Such activities include sector-wide planning, development of sector best practices, sector-wide promulgation of programs and plans, development of requirements for effective information sharing, research and development, and cross-sector coordination. Information sharing is focused on delivering alerts, warnings, and advisories to the sector.

Where Do We Stand in the Development of Such Partnerships?

Security readiness is a long-term proposition. To get there, the U.S. will migrate through three stages:

- Evaluation – wherein we seek answers to the new security paradigm for the homeland

- Adaptation – wherein we take initial steps to organize our homeland security program
- Transition – wherein we build the homeland security program, measure its effectiveness, and continuously reduce risks to America from terrorist attacks

As part of this evolution, we will see that public-private partnerships have emerged as critical elements of our homeland security strategy. Ultimately, they will play an even greater role as we implement it.

Evaluation. Prior to September 11, 2001, the nation as a whole had very little appreciation of the threats to our homeland. Matters of national security were handled largely at the Federal level, within all three branches of government, and among a multitude of agencies that operated largely independently. Given these circumstances, few would argue that there was meaningful interaction, much less partnership at the Federal level. Even less interaction occurred at the State level. Locally, public and private owners and operators of CI had just begun to organize themselves around security issues.

In the three years since that tragedy, we have made considerable progress toward both understanding the need for partnerships and in initiating some key partnership arrangements, particularly in the area of information sharing.

Progress to date, however, is far from complete, which is not surprising given that fundamentally we are just beginning to evolve along this natural progression of change. This process began with 9-11, where in the immediate aftermath, America was preoccupied with evaluating the new security paradigm:

> What does it mean now that we realize that we can be attacked on our own soil?

In fact, 9/11 changed everything and through the process of evaluation, we learned just how serious the new security paradigm was.

Adaptation. Arguably, the creation of DHS and DHS's subsequent organization of the nation's homeland security program through creation of NIPPs as described above, marks the beginning of the second stage—adaptation. One of the fundamental realizations during adaptation is that effective and efficient homeland security will require cooperation

between the public and private sectors at a scale never before contemplated or attempted.

We are now in the latter stages of this adaptation process. The DHS's National Infrastructure Protection Base Plan recognizes this, but nonetheless, boldly calls for a broad range of partnerships as the key delivery mechanisms. Not surprisingly, each of the seventeen sector-specific plans also call for such partnerships, although at the sector scale, the nature and scope of partnerships varies considerably from one sector to the next.

Transition. Over the remainder of this decade, we will see just how well the nation does at meeting our homeland security objectives. There is much still to debate, not the least of which are a critical series of issues surrounding how the private sector partners with government agencies effectively. With national defense as our closest model, it is natural to expect government to act unilaterally on behalf of all Americans. But in homeland security, as argued earlier, this simply is not possible: CI systems are too complex, too interconnected, too diverse, and owned and operated too heavily by the private sector.

Partnerships among government agencies, between different levels of government, and between government and the private sector are needed to make this transition effective and efficient. But how will we deal with confidentiality of information? How will we deal with traditional command and control relationships between government and private infrastructure owner/operators? How will we harness market forces to drive private firms to be profitable and implement national security objectives?

Policy Implications as the Nation Transitions to "Partnership Readiness"

As the owners and operators of the majority of CI assets, private sector firms engage in risk management planning and invest in security as a necessary business function. They also remain the first line of defense for their own facilities. In implementing the NIPP, private sector owners and operators will be called upon to follow their own sector-specific infrastructure protection plans and work with DHS, and other Homeland Security implementation partners, such as State and local agencies to identify and implement best practices, develop performance

metrics, develop information sharing mechanisms, and ensure cross-sector coordination.

But private owners and operators of CI also have responsibilities to their shareholders who expect a return on their investment and to consumers who enjoy their products or services. Fundamentally, these obligations must be met above all others, since without consumer demand, reasonable profits, strong cash flow, and a healthy balance sheet, there simply will be no private sector with whom to partner. It is in everyone's best interest—government and the private sector alike—to find ways to engage the private sector in the transition to a secure America while maintaining their integrity in the private economy.

Fortunately, there are solutions—*if we pay attention to a few key policy principles; all of which can be further refined through the partnerships we have already begun to form:*

- Rely to the greatest extent possible on the market to guide private security decisions
- Focus on consistency of security outcomes and enable both governments and private owner/operators to achieve these outcomes in the most efficient and effective way
- Especially in sectors with a high proportion of private ownership and operation of assets, promote flexibility to accommodate the diversity of conditions from one owner to the next
- Where government is involved, eliminate to the greatest extent possible, hierarchical decision structures and promote independent, entrepreneurial thinking
- Support local readiness, response, and recovery actions by eliminating barriers to innovation and cost recovery, not necessarily by funding security improvement directly
- Measure progress against outcomes and hold accountable, those with the authority to enact changes

Protecting the homeland is a long-term proposition. In the new security paradigm, in fact, our job is never complete since threats will change, as will our own vulnerabilities. Government, academia, and

private infrastructure owner/operators must be prepared to participate as partners in a continuous process of improvement in homeland security.

Figure 2 is one model of such a process integrating a comprehensive set of processes together to form an active and effective platform for securing infrastructure assets within a risk management framework. Roles and responsibilities of government agencies, private owner/operators, and others like academics and research institutions may change somewhat to accommodate unique circumstances from one sector to the next, but by and large, this process can be applied across sectors to guide the nation through its transition to the new security paradigm. At the expense of over-simplifying many very complex processes and decisions, I will offer my own thoughts on each step.

Figure 2: Securing Infrastructure Assets Within A Risk Management Framework

Threat Definition. The process begins with a threat definition step, which thankfully in many sectors, we have already made considerable progress. As DHS continues to mature and tools such as the HSIN are more fully developed, the threat definition process will only strengthen, as will our ability to communicate reliably and thoroughly as threats change. The key to this step, however, is consistency, without which individual owner/operators may remain vulnerable despite actions they may take based on their own views of threats. This implies that government take a lead role in assembling historical data on threats, gathering current intelligence, interpreting these inputs, and articulating a consistent profile of threats for each CI sector. Sector representatives, perhaps through the new SSCs to DHS, should validate national threat assessments and perhaps define local threats where appropriate. Government's role also includes threat communication.

Risk Tolerance Thresholds. These are sector-specific and where consequences of a terrorist attack can be expected to be localized, risk tolerance decisions can be similarly localized. Basic assumptions in setting such tolerances are that risk can be reduced, but not eliminated, by reducing the probability of an attack, the probability of it succeeding should one occur, and the consequences should an attack be successful. Since risk tolerances are largely related to social expectations, including those of consumers and investors, key stakeholders should be involved in defining them. Risk tolerances will be important inputs to the validation step.

Risk Assessment Methodology. Again, most sectors have made considerable progress creating risk assessment methods and many have applied and refined them widely across their sector. Funded and sometimes shaped at the Federal level (where consequences of an attack could have national implications, as would be the case, for example in nuclear power generation), research institutions and universities have played a key role in this regard. Most methods incorporate the following steps: characterization of the assets to be protected, characterization of the threats to be protected against, assessment of vulnerabilities of these assets to the threats, forecasting of consequences of asset failure, and prioritization of risks (Vulnerabilities times Consequences) across assets. While these assessments are generally executed by infrastructure owner/operators, there may well be a need to accumulate risk knowledge

across the sector to facilitate a national-scale assessment of risk so that we can track progress, allocate resources, and create targeted risk reduction interventions for the highest priorities.

Good Practices Toolbox. The toolbox needs to contain risk-reduction solutions that meet a wide range of circumstances from one sector to the next and from one entity to the next within a sector. Consequently, some tools will be sector-specific while others may be more globally applicable. Tools should be designed to produce one or more of the following three types of outcomes: reduced probabilities of attack, reduced vulnerabilities to an attack should one occur, and reduced consequences of asset or mission failure should an attack be successful. Research institutions, private suppliers of security solutions, and individual asset owner/operators play the key role here. But the government may have a role to play in funding research and/or organizing and funding mechanisms to accumulate and share knowledge with sector users about tools and their effectiveness.

Risk Control Processes. The extent to which any infrastructure owner/operator implements risk controls must be a local decision based on balancing broad homeland security goals and private responsibilities to shareholders and customers. Where infrastructure failures can have national effects, balance should be tipped toward broader homeland security objectives. In any case, risk control measures are designed to deliver detection, delay, assessment, response, recovery, and knowledge sharing.

Validation. Validation is needed in the process to ensure accountability for risk reduction actions, whatever they may be, and is a precursor to cost recovery. Validation processes will surely vary from sector to sector, but inevitably will involve some government participation (to protect the public interest) as well as the participation of industry experts. Validation checks for whether and the extent to which solutions are effective, sustainable, and prudent.

Cost Recovery. This is a critical step, especially for private owner/operators and especially where prices and/or quality of services they deliver are regulated or controlled by non-market mechanisms. Examples include the traditional utility sectors like water, energy, and telecommunications. Where agreed risk tolerances have been adopted and risk management

actions have been validated according to these tolerances, cost recovery should be uncontestable and rapid.

Sustain, Maintain, and Learn. Partnerships are key to this step to promote knowledge sharing, learning, and adjusting. Based on what we learn, how we cycle through each of the other steps can be expected to change. Government's role is to organize and possibly fund processes and programs within and across sectors to assure that these objectives are met. Information security and confidentiality concerns must be addressed.


Prudens
Futuri

Sticks and Carrots: Incentives and Regulations for the Private Sector

Al Martinez-Fonts

Special Assistant to the Secretary
Department of Homeland Security

There is still, after a year and a half, some misunderstanding as to what the Private Sector Office of the Department of Homeland Security (DHS) does. The Private Sector Office is a unique position; the Departments of State and Commerce have something similar, but nothing with the unique mandates given to our office in DHS.

First and foremost, the Private Sector Office is a staff position, not an operating unit. Many of us come from a business background, and coming from that background, one of the first things we do is try to diagram the business in order to figure out how it works. The Department of Homeland Security has seven operating divisions. Three of these organizations you have known and loved for years: the U.S. Secret Service, which has been doing its job for almost a hundred and fifty years; the U.S. Coast Guard, who have been doing their work for almost two hundred years; and Citizenship and Immigration Services, which processes the thousands of people who come here every day. What has been recently created are the four new pillars of Homeland Security: the Under Secretariat for Information Analysis and Infrastructure Protection (IA/IP), which provides us with continual input on the threat and on our vulnerabilities; Border and Transportation Security, which includes 120,000 of the 180,000 personnel in DHS, working in Customs and Border Protection, the Transportation Security Agency (TSA), Immigration and Customs Enforcement and numerous other law enforcement entities; Science and Technology, which is basically the "Underwriters Laboratory" for DHS, testing new technology as it is developed to combat the threat; and Emergency Preparedness and Response, people who have been doing disaster response for years and years—primarily through the Federal Emergency Management Agency (FEMA)—and now are growing to bring that expertise to bear in response to damage caused by weapons of mass destruction.

Those are the seven operating units of DHS. Within DHS, however, there are several staff offices that serve the entire organization. The Private Sector Office is one of those staff offices. Primarily, the mission of the Private Sector Office, first and foremost, is to act as an advocate for the private sector. Given that approach, we sometimes have a hard time keeping the vendors away, although we do actually try to help vendors to ensure that they can make contact with the right agencies. However, what is far more important is that we listen. We listen, for example, to the insurance industry as they bring us their concerns, most recently about the Terrorism Risk Insurance Act. We listen when private industry tells us that some DHS policy, response, or program is going to place a huge financial burden on some element of the private sector, be it an entire business sector or one business. If we shut down the private sector, the terrorists have won. It is my job to bring that feedback to the Secretary. Oftentimes, in some tabletop exercise, the decision will be made to close some major facility; for example, O'Hare airport. It is my job to look at the potential economic impact of that decision and let the Secretary know that shutting down that airport could have a devastating economic effect far beyond the possible impact posed by the threat.

Our second function is to share: to share information and best practices. It is our job to take the information being developed—for example, in IA/IP—and make sure that it gets out to the private sector in a timely manner and in a form that they can use. Much of the information generated by the Department is focused on critical infrastructure, and while the list of things considered to be critical infrastructure grows daily, Wal-Mart, the largest retailer in the United States, is not critical infrastructure; neither are General Motors, Ford, and Chrysler. Critical or not, we still need to keep those corporations informed, not to mention the millions of small and medium-size businesses that are scattered throughout the country and are so critical to our economy. According to the U.S. Chamber of Commerce, there are 25 million businesses in America; there are fifteen people in the Private Sector Office. Obviously, we have to split the requirement up. We work very closely with trade organizations. And whether it is the U.S. Chamber of Commerce, the Business Roundtable, the National Federation of Independent Businesses, or others, we work hard to get the information out to those organizations that can then pass the word on to their members.

The second part of information sharing is the sharing of "best practices." Why do we need to reinvent the wheel? Yes, sometimes, sharing at this level, we do have the problem that best practices tend to become the lowest common denominator, and that is not what we want. We truly need best practices. Once again, our strategy is to split the requirement up; we cannot treat the corner drycleaner the same as a major manufacturer, but we still have to reach out to them. It is a huge challenge, but we have to take it on.

Our third function, one that is specifically mandated by the law, is the creation of public-private partnerships. Former Deputy Secretary Gordon England used to say, "when you have a problem, the last thing you want to do is dial a telephone number that starts with 202" (for anyone who does not know, 202 is Washington, D.C area code). You want to call 911 and get a local response. Even if you are EXXON Mobil, your local chief of security's first link needs to be to the local police. Now the corporate head of security for EXXON Mobile may want to have a link to IA/IP, and to our office, but that first linkage must be local. We are trying to ensure that those links are there, and that they are strong.

The final function, one that I am certain is near and dear to all of you, is looking at those economic consequences. If we kill the goose that lays the golden eggs, we know how the fairy-tale goes, and we know what will happen. If we choke the private sector, if we stop commerce and people from coming into our country, we will have lost the war against terrorism.

The primary goal of the Private Sector Office is to prove what we call the "business case" for homeland security. We believe that the money a company puts into security ought to be viewed as an investment, not as an expense. While sometimes it is very difficult to prove that spending money on "guns, guards, and gates" will provide a return on investment, we believe we can make that case.

When we talk about crossing our borders, whether it is a truck or just one person, we cannot afford to have just speed in the crossing process, or just accuracy. If we were to open up the border with Mexico, to just let every truck through, we could expose ourselves to innumerable threats, weapons of mass destruction and lots of bad people. Neither, however, can we afford to stop and search every truck. If you have ever seen a

tractor-trailer rig taken apart and searched by hand, you know how lengthy and detailed a process that is. It would kill commerce. To meet the challenge of providing both speed and accuracy, we have come up with programs like the Customs Trade Partnership against Terrorism (CTPAT) and FAST (Free and Secure Trade), which provide special lanes through customs. It used to take Delphi an average of three hours to go from their plant in Juarez to their distribution location in El Paso—that is about ten miles.[1] At that time, the wait at the bridge over the Rio Grande could take anywhere from fifteen minutes to ten hours. Since then, Delphi has joined CTPAT, which means we go into their plants, check their processes, and check their people. As a result, Delphi's trucks can now use the FAST lanes, and they are now moving across the border considerably faster than before. Since opening the FAST lanes in El Paso, the average time to make that trip has dropped to forty-five minutes. The wait at the bridge takes from fifteen minutes to an hour and a half. Think of the savings, from a business perspective, in terms of fuel, wages for the driver, and use of the truck—not to mention the environmental benefits and the reduced impact on everyone else trying to use that bridge. Delphi has told us that if we can open a FAST lane at Nogales Arizona, we will save them $100,000 a month. That is what we mean by fast and secure trade. We hope to open that lane this year or early next year.

There are numerous other examples. As a result of the 24-hour rule, K Line can now issue a bill of lading in eight hours, rather than two and a half days.[2] According to the people at the Port of New York, pilferage has dropped 45 percent since 9/11. Pilferage is reported to be an eight to twelve billion dollar industry. Reducing that by 45 percent (at least in New York) is an incredible economic windfall.

In accordance with the Maritime Transportation Safety Act, every commercial vessel over fifty-five feet must have a transponder. The purpose of the legislation was to be able to locate these ships in the ports.

[1] Editor's Note: Delphi Corporation is one of the largest auto parts manufacturers in the world. It was spun out of General Motors and was formerly known as the Delco Division of GM. It is a publicly traded company.

[2] Editor's Note: The 24-hour rule refers to the advanced manifest requirement. DHS now requires that the manifest for goods to be shipped into the United States be sent to Customs and Border Protection 24 hours in advance of the cargo transiting the border. Kawasaki Kisen Kaisha, Ltd. ("K" Line) is a global transportation company linking the Pacfie Rim with North America and Europe.

The insurance industry has been able to lower rates based on this capability, not only to locate the vessels in the ports, but also to locate them on the high seas. This facilitates repair, rescue, and safe routing. Investing in security leads to returns on the shipping companies' insurance bills. If we can make a business case, using examples like these and countless others, I believe that the private sector will be willing to pay for enhanced homeland security.

Even given that, I still believe that the government does not understand the private sector, and the private sector does not understand the government. We need to bridge that gap. We can appeal to patriotism, but patriotism will only get us so far. We need to understand that the government may be driven by security, but the private sector is driven largely by profitability. Our basic operating principle must become that by working together, we can achieve both.

We must present private industry with a value proposition. I believe that the private sector is looking to the government for leadership and direction, but the private sector wants to execute on its own. We need to emphasize best practices and standards. Best practices should be the preferred approach—voluntary, not regulatory—where there is more flexibility in development and implementation. However, there will be times where the requirements are such that standards and regulations will be necessary. Chlorine tanks, in my opinion, are so scary that we do not want to leave it to just anybody to figure out how to deal with them. In cases such as that, we may have to mandate standards; but in general, best practices are a better approach. The insurance industry is contributing to this process by evaluating best practices and offering incentives for those who apply them.

An important element of this value proposition is the value of information sharing. The government has a tremendous amount of information; many regard us as the preeminent source of information. However, we have a bit of paranoia about sharing this information with the private sector—especially sharing with people without clearances. Do we need to work on the clearance process? Do we need to have a process to "dumb down" the information so that it does not require a clearance—a sanitizing process? Obviously, access to this information can be valuable to the private sector. What many do not realize is the value of

the information that the private sector can provide to the government—in terms of databases and in terms of situational awareness.

Another thing that much of the private sector is looking for is some relief from liability.[3] I am not sure that it is possible; neither am I sure that we want absolute relief from liability. One of the many rights that make this country so great is the right to sue, but we need to put some kind of limitation on this thing so that the threat of litigation does not prevent the private sector from doing what needs to be done in terms of advancing domestic security. Take, for example, an effort by a company to produce some vaccine, or devise some new tool for security. If a company knows that there is a chance that their products might misfire one time in a million, and that resulting lawsuits could put them out of business, those security efforts are risks they might not be willing to take. Not taking those risks, not developing those new products, not introducing those new concepts, may be to the detriment of us all.

From a wholly different perspective, the Private Sector Office and the Private Sector Senior Advisory Committee (a group of about a dozen CEOs and senior business leaders from around the country who advise the Secretary) have identified Visas as the number one "security-related" cost to business in this country today. The inability to get people into this country so that we can sell them our products is having a massive effect. In that regard, the government is creating a tremendous inefficiency.

As a final note, I would like to offer an example of how "enhanced security measures" can adversely impact the "most private sector"—the individual taxpayer. I recently re-financed my home. Now, I was a banker, so I know all about the mountain of paperwork required for this process. As I was working my way through all of this, I encountered a $120 "U.S. Patriot Act and other fees." Naturally, I inquired what this was for. The response was that these fees were to defray the costs of the background checks mandated by the Patriot Act. Before the Patriot Act, background checks had cost about $50; they had gone up by $70. I gave this information to an economist in our office who estimated, if you assume that every homeowner has a mortgage, these background checks are costing the American public $655 million dollars a year. Now

[3] Editor's Note: In the interests of full disclosure, Mr. Martinez-Fonts noted that he was the First Chairman of San Antonians Against Lawsuit Abuse.

I recognize that not everybody has a mortgage, but this number is at least illustrative, and the condition it represents is simply unacceptable.

We can do better, and we must do better. The efforts we are making in information sharing, in creating public-private partnerships, in new initiatives like CTPAT and FAST, and in understanding the consequences of our actions for the country's economy, all contribute to improving homeland security. The U.S. economy is a primary target of our enemy. If we build on our efforts to date, and if we successfully make the case to the private sector that every dollar they spend on enhancing security is an investment and not just a cost, the private and public sectors working in cooperation can defeat the enemy and frustrate their plans.


Prudens
Futuri

Breaching the Trust Barrier: Information Sharing For The Common Defense

Harrison D. Oellrich

Managing Director,
Guy Carpenter & Co., Inc.

It is an honor and a privilege to be asked by the Army War College to join with it by participating in the important undertaking of enhancing our nation's critical infrastructure via public-private collaboration, particularly as it pertains to the sharing of salient information and data.

I must admit that writing for such an accomplished group outside of my specialty is a bit outside of my comfort zone, since I am not a military officer, nor a scientist, technologist, academician, engineer or member of our government. What I am is a businessman, and a reinsurance intermediary by training. I represent Guy Carpenter, the world's largest and preeminent reinsurance intermediary. Prior to the attacks of September 11, Guy Carpenter's home office was located on the 49th through 54th floors of Two World Trade Center, so it is easy to understand that as a firm and as individual citizens we have every reason, both from professional as well as personal perspectives, to assist with the absolutely critical Homeland Security process however we can.

So how, of all things, can the insurance sector play a key role in the process of protecting the Nation's critical infrastructure? And what is "reinsurance" anyway?

Reinsurance is probably a term that you have come across only rarely, if ever. However, it can be the key driving force behind the availability and affordability of insurance coverage to most enterprises within our economy. Without insurance the risk of doing business from a whole spectrum of potential threats, from perils both natural and otherwise, would, for many companies, their investors and shareholders, be unacceptably large.

All insurers, from the most modest single county mutual insurer right up to and including the largest multinational stock company, require various reinsurances. At the end of the day, most of these are

purchased to provide an insurance company with one or more of the following benefits—capacity, stability, financing, and/or protection from catastrophes—and are sold by reinsurance companies or reinsurance departments of insurance companies throughout the world. Some of the more prominent reinsurance companies include Lloyd's of London, General Re, American Re, Munich Re, and Swiss Re; and there are many others.

Over the past decade, insurers and reinsurers have spent a tremendous amount of time and resources in an effort to quantify, through the use of increasingly sophisticated probabilistic and deterministic modeling, the actual expected losses to either their existing portfolio or a theoretical portfolio of risks in catastrophic loss scenarios. These scenarios include earthquakes, windstorm, hurricanes, or other physical peril. Having convinced themselves that they can thus construct a portfolio from which they can expect an acceptable exposure to loss from natural perils, along come new exposures—to terrorist acts never before contemplated—that appear to subvert their risk management protocols.

Accumulations of exposures that were never thought to correlate have been identified by the events of September 11. Many insurers and reinsurers have noted that the number, kinds, and values of losses occasioned by 9/11 are similar to those their models predicted would result from an earthquake in California occurring during working hours. However, no one would ever have contemplated the magnitude of loss resulting from a terrorist act against an office complex in New York City or its collateral losses.

Similarly, in recent years, exposures associated with cyberspace have quickly emerged. Insurers (especially reinsurers) have become increasingly concerned that, inasmuch as these very sophisticated exposures were never contemplated, they cannot be successfully underwritten, especially within the context of traditional bricks-and-mortar property and casualty policy forms.

As a result, a new generation of insurance products focusing solely and specifically on these exposures has been developed, and they are already undergoing considerable refinement. Since they are stand-alone products, they allow underwriters to have the opportunity to individually assess, underwrite, and price each insured's unique Internet exposures.

This, in turn, should make these products more attractive to prospective reinsurers.

However, for this marketplace to ever have the opportunity to reach its incredible potential, data, and methodology to model such available data, will have to be developed to allow both insurers and reinsurers to have the confidence necessary to build these new portfolios.

The Internet is unique in that, on the surface at least, it seems to defy modeling. Whereas losses from natural perils occur in a specific geographical location, the Internet is both everywhere and nowhere at the same time, and the perils to be protected against are still being fully identified and defined.

Consequently, in order to address the aggregation issue a means of slicing and dicing the Internet, in a fashion similar to the way traditional property catastrophe exposures are done, needed to be developed. Having done so, we hope to have provided a framework for a future ability to model these emerging exposures, so that insurers and their reinsurers will not need to aggregate every dollar of exposure from this class with every other future dollar of exposure they will put on the books. Our initial efforts have been well received by worldwide property catastrophe reinsurers, who have fully subscribed to the first "Cyber Hurricane" Catastrophe reinsurance placement completed on behalf of a major client.

Data needed to populate insurers' and reinsurers' models for bricks-and-mortar property catastrophe exposures is plentiful, while historical data to build and run future models for these new exposures is virtually non-existent. In point of fact, many past attacks have never even been reported. Companies are fearful of sharing information about cyber crime and attack, since their reputations can be seriously damaged if customers believe on-line transactions may not be secure.

With credible data and a way to model the exposures, there is every opportunity to build a substantive and sustainable reinsurance marketplace to support these products for insurers, reinsurers, and their respective clients. To that end, Guy Carpenter and other sector leaders have been working closely with various components of the Federal government as part of a series of joint public-private collaborative efforts that are designed to strengthen network security.

Since government utilizes the net in the very same way as the private sector, the Internet has been designated as one of the key components of our Nation's critical infrastructure. It must be protected from attack at all costs.

That said, it is obviously in the government's interest to support our sector's efforts to develop a working marketplace for these exposures, as they have recognized that the disciplines that the marketplace can provide are exactly the same as those the government wishes to impose. However, since the government doesn't own or control the Internet—and given the fact that the Administration would likely be loath, from both a philosophical as well as a political perspective, to impose regulations on it even if doing so were feasible—some other mechanism must be found to encourage network infrastructure owners and operators to harden their own networks. Insurance can be one such mechanism.

An analogy useful to understanding the dynamics at work here is as follows. The owner of a factory or plant doesn't necessarily install his fire detection and suppression or intrusion systems to protect his plant, machinery, and inventory out of some higher sense of altruistic virtue. The owner does so in order to qualify for, obtain, and/or be able to afford the insurance coverage mandated by his creditors. So, too, can the owner of a network be "incentivised" to harden his network environment in order to qualify for or obtain affordable insurance coverage. The resulting outcome is a more secure network environment over time, with the resultant decrease in vulnerability to attack.

Consequently, we hope to be able to share data gathered by various governmental agencies, and perhaps even to explore methodologies they use, to model similar exposures and apply lessons learned. Single points of failure, cascading interdependencies, and the like are all important to understanding the potential for catastrophic loss posed by these new exposures. If government has delved into these thought processes and is able to work together with us to mine, massage, and model data in this regard, then there is no reason that a robust, substantive, and sustainable marketplace cannot be created.

If, as those of us active in building this initiative within our sector say, "networks are the buildings and automobiles of the 21st century," then before very long a working insurance marketplace can be built to

support the emerging exposures of cyber space. By extension, a stronger market place will make the Nation much more resistant to cyber attack or cyber terrorism. For a greater understanding on the direct role of the market place in these regards, I would recommend Ty Sagalow's article, "The Role of Cyber Insurance in Fighting the War on Terror." Mr. Sagalow is the Deputy Chief Underwriting Officer for American International Group (AIG) and a thoughtful leader in the development of this emerging marketplace.[1]

Even before the 9/11 attacks, we had been engaged in the quest for cyber security via a series of collaborative efforts with the executive and legislative branches of the government designed to create a new segment in the insurance marketplace for companies transacting business over the Internet. By creating *better* practices in network security (who knows what "best practices" will ultimately develop?), a more hardened network environment can be attained, contributing to the entire Nation's defense against the potential threat of cyber attack or cyber terrorism.

So we at Guy Carpenter, along with other elements of the insurance/reinsurance sector, have had several years of insight through these initiatives in which to see the opportunities as well as the challenges presented in undertaking collaborative work with the government. Our experiences may serve as proxy for what are likely to be many other efforts undertaken and stepped up as a result of the new sense of necessity and urgency regarding collaboration in our post 9/11 world.

What have we learned from our efforts? It seems to be clear that there are at least three separate and distinct ways that government can influence the private sector to maintain and enhance behaviors designed to contribute to national security. The government can either:

1. Mandate (by regulation) that the private sector undertake certain actions in the national interest;
2. Coax and/or cajole the private sector into doing so; or preferably,
3. Provide incentives to the private sector to undertake actions deemed necessary in the interest of the national security.

[1] Mr. Sagalow's article is contained within this chapter, re-printed with his permission.

By way of the third alternative, the private sector can conceptualize, create a business case for, and then embrace actions necessary to promote national security in a way that truly becomes a "win/win" approach. The private sector generates revenue (and hopefully profit) by undertaking measures that are in the government's interests anyway, while simultaneously fulfilling our obligation to shareholders and enhancing value for our investors.

So let's take a look at our scorecard of successes in working with the government to date and examine the obstacles and challenges that we have identified in doing so. First with respect to successes:

- Just the fact that we are here today thinking and speaking about this sort of collaboration, and that institutions like the Army War College are ferreting out contacts and soliciting the views of representatives from within various components of the private sector, is a success in and of itself.
- Since reaching out to the government, and the government's reaching out to us, a significant network of contacts has been established that can be called on when needed. This has begun relationships that will be vital to making things happen when the chips are down.
- Ongoing symbiotic efforts like those discussed here will prove mutually beneficial for both the government and the private sector. As success breeds success, additional initiatives and cooperative efforts will take place in the future.

There have, of course, been a number of challenges encountered in initiatives undertaken thus far:

- There is nothing helpful about the constant ebb and flow of players within government who engage, and then lose interest in issues of ongoing importance to the private sector in response to the political environment. This inconsistency was exacerbated by the re-organization of myriad agencies, offices, etc. that occurred when the Department of Homeland Security was created and a whole network of contacts who were working these issues was lost.
- A similar problem will likely occur any time a new administration takes the reins in Washington, as political appointees depart and must be replaced by successors who

must educate themselves on issues, initiatives, and contacts generated with the appropriate stakeholders.

- The cultures, and even the language used by the government, the military, and the private sector are so different that it is sometimes difficult to communicate and to understand one another. The sense we have is that we have been working in parallel universes for many years, and while common goals have been set, figuring out how to make things happen is still very much a work in progress.
- While relationships are building, and with them trust between representatives of the government, the military, and the private sector, the issues of what can be shared and how it can be shared are still significant impediments to moving the ball. The process for obtaining requisite background checks and security clearance needed to work with classified materials is labor intensive, expensive, and a bit intimidating. The private sector is not blameless here either, in that we oftentimes are extremely reluctant to share proprietary information for fear that it could find its way into the hands of competitors, or perhaps even be used against us by an overzealous government.

So, where are we in building the trust necessary between the government, the private sector, and the military to be truly effective in working together for the Nation's common good? From our perspective we have made an excellent start; but given the threats faced today from a very nontraditional but totally committed enemy, there is every reason to continue to build on this start and to accelerate our efforts to work smoothly together to make our Nation a safer place for all of us to live.


Prudens
Futuri

The Role of Cyber Insurance in Fighting the War on Terror

Ty R. Sagalow[1]

Chief Operating Officer and Executive Vice President
AIG eBusiness Risk Solution

Introduction: Removing Uncertainty from the Equation

The campaign against terrorism is being fought on many fronts, including cyberspace. And in this most unconventional battle, attackers can be expected to use every tool available to them, including the Internet, to breed fear and chaos, to threaten our national interests, and to ubiquitously breach our borders, both on land and online. Yet the enemy's fear-based campaign can be attenuated to the extent that we remain one step ahead, and remove uncertainty from the equation.

Fortunately, efforts are now underway to raise awareness to the need to more rigorously defend the Nation's cyber borders. The government and private sector have joined forces to promote the universal need to leverage more effective information security risk management technologies and practices, including cyber insurance, to prevent and mitigate the damaging impact of potential cyber attacks.

Internet Adds Dimension to New Virtual Battlefield

Ironically, the Internet was developed in the 1960s under the leadership of the U.S. Department of Defense as a decentralized military

[1] The views and policy interpretations expressed in this work by the author are his own and do not necessarily represent those of American International Group, Inc. or any of its subsidiaries, business units or affiliates. No policy interpretation contained herein should be relied upon by any person in the interpretation of that person's insurance policy. Persons should always seek the advice of counsel or a professional insurance broker before purchasing any insurance product.

Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions. Coverage may not be available in all states. Issuance of coverage is subject to underwriting. Non-insurance products may be provided through independent third parties.

communications network that could withstand a cataclysmic attack.[2] It has since evolved into a vast global network of interconnected computers that individuals and businesses now use to exchange information and conduct business transactions online. This same omnipresent connectivity adds a new, virtual dimension to the enemy's battlefield, enabling them to invade from limitless rally points, and causing a staggering untold sum of damages to date.

The pace of innovation has not been met, and in all probability can never be met, by sufficient technology standardization and implementation necessary to ensure 100 percent reliability in end-to-end network and systems security. Indeed, cyber threats are ever changing; and as soon as a security solution is introduced, increasingly sophisticated perpetrators seem to find a workaround.

It's no secret that gaping security holes exist within the public and private global network infrastructure, and recent attacks have borne out this unfortunate truism. In late 2002, for example, the nefarious Bugbear virus crippled worldwide computers in the year's most severe computer attack.[3] And industry sources estimate that the total damages from cyber attacks resulting from malicious code may have been more than $13 billion in the year 2001.[4]

Cyber terrorists have exploited such vulnerabilities to steal information, such as individual identities. The Federal Trade Commission cites identity theft as the leading consumer complaint in 2001 by a wide margin,[5] and the growing problem can have grave consequences. Using stolen identities, terrorists can fund their operations and damage American interests. For example, in June 2002, a chilling case of online identity theft was revealed in which an individual's credit card information was used through confidential online transaction broker ccnow.com to buy a range finder, which calculates the distance to an intended target, and a Russian-made night-vision rifle. The cardholder revealed the fraudulent

[2] "Founding Father," by Stewart Brand, Wired Magazine issue 9.03, March 2001.

[3] Dow Jones Newswires, October 6, 2002, "Severe Computer Virus Spreads, Lets Hackers Steal Info."

[4] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace,* draft for comment, September 2002, page 3.

[5] Federal Trade Commission, January 23, 2002 press release, "Identity Theft Heads the FTC's Top 10 Consumer Fraud Complaints of 2001."

charges and the charges were reversed, but not before the weapons had shipped to an unidentified criminal in Saudi Arabia.[6]

Need for Risk Management Takes on Added Urgency

The government is now redoubling its efforts to address vulnerabilities in the national information infrastructure, forming the President's Critical Infrastructure Protection Board (PCIPB) within the Executive Branch, and including the Critical Infrastructure Assurance Office (CIAO) as part of the Homeland Security division of the Department of Commerce.

In mid-September [2002], PCIPB issued for comment a draft proposal,[7] "National Strategy to Secure Cyberspace," supplementing the *National Strategy for Homeland Security*, and the *National Security Strategy of the United States*. The PCIPB strategy strongly calls for a risk management approach. It notes that "the tools of destruction are broadly available, and the vulnerabilities of the Nation's systems are many and well known. These factors mean that no strategy can completely eliminate risk, but the nation can and must act to manage risk responsibly...."

The urgent need to manage cyber risk more responsibly stems from the fact that security breaches can target not only information but also the Nation's critical infrastructure (utilities, transportation, water, financial services, etc.), which is also inextricably tied to and dependent upon information technology. The drafters of the National Strategy made the same foreboding observation: "…cyberspace security is not about 'good ones and zeroes attacking bad ones and zeroes.' It is about whether when one throws the switch, the electricity comes on, or whether the money Americans have invested and deposited is there, and whether this country is secure."

Lack of Public Awareness Fails to Rally an Effective Defense

The War on cyber terror would perhaps benefit from a full-press public relations campaign, since the challenge of combating an invisible

[6] Christian Science Monitor, June 05, 2002, "Our Man Ordered Waffles, But Paid for Tools of War."

[7] When this article was originally published the proposal had not been issued in its final form, therefore the content of the final report may vary from that described herein.

foe is exacerbated by the fact that many Americans have yet to grasp the scope and severity cyber threats pose. With computer attacks, no gunshots are heard, no chilling news footage is aired to alarm and rally the public, as in the devastating events of 9/11.

As a result, "netizens" feel a false sense of security online. Government and business leaders have thus begun the present coordinated effort to educate the public and private sectors about the new cyber threats and solutions available to combat them. The hope is to mobilize citizens on all levels of society to thwart cyber invaders who seem intent upon establishing a virtual beachhead.

Both individuals and companies can weaken the broader effort against cyber attackers by failing to take reasonable safeguards. For instance, individuals who fail to implement personal firewalls and anti-virus security software on their home computers can suffer financial damage personally, such as having their personal information stolen, or their computer damaged. Without proper safeguards, that individual may spread a virus to countless other users, exponentially increasing the damages, rather than heading the attackers off at the pass. Worse still, their stolen information may fall into the wrong hands, to the benefit of the adversary.

The proposed National Strategy outlines proactive measures individuals and businesses can take—a blend of 1) technology investment, 2) human controls, and 3) financial protection—to reverse the troubling trend of cyber terrorism. Using this blended risk management approach, individuals and businesses should assess what security technologies, procedures, and human controls they have in place and address vulnerabilities by implementing appropriate safeguards. For example, firewalls and anti-virus solutions will do little good if employees within an organization are not properly educated on security risk management technologies, policies, and practices.

After a risk assessment, individuals and businesses should take the necessary steps to prevent and mitigate the impact of potential cyber attacks, using a combination of technology, processes/procedures, and human resources. Individuals and businesses should then consider tools such as cyber insurance to transfer financial risk and retain the balance of risk that cannot be prevented, mitigated, or transferred. Taken together, these five tools, as shown in figure 3, represent a complete approach to risk management.

Risk Assessment	Analyzing the potential likelihood and the potential impact (financial and non-financial) of cyber attacks.
Risk Prevention	Taking the most preventive measures possible within their means to reduce the likelihood of a successful attack, leveraging a blend of technology, processes/procedures, and human resources.
Risk Mitigation	Reducing the potential financial loss arising from a cyber attack that cannot or are not protected.
Risk Transfer	Transferring to others the financial loss that remains after steps have been taken to assess, prevent and mitigate risk. This can be done through contractual "hold harmless" indemnification provisions, for example, or insurance.
Risk Retention	Retaining that portion of financial loss as the result of financial risk management analysis to determine that financial loss which could not be reasonably prevented, mitigated or transferred. Following a comprehensive risk assessment, this is the net financial loss that remains after risk prevention, risk mitigation, and risk transfer strategies are successfully implemented.

Figure 3: Tools for Effective Cyber Security Risk Management

The campaign on terrorism cannot succeed without the adoption of comprehensive risk management controls at all levels of society. After all, the Internet is, by definition, a global network of digitally connected computers, the shared responsibility for which lies in a combination of public and private hands.

The Role of Insurance in Managing Cyber Risk

The National Strategy acknowledges the key role insurance can play in combating cyber terrorism and the need to "work with the insurance industry on ways to expand the availability and utilization of cyber security insurance."[8] Likewise, the widely referenced 2002 CSI/FBI Computer Security survey of international security experts notes for the

[8] The PCIPD, *The National Strategy*, September 2002, Recommendation 2-5(d).

first time that companies for which eBusiness exposure is particularly high should consider eBusiness insurance.[9]

The Banking and Financial Sector as well as the Insurance/ Reinsurance Sector concurred in their recommendations to the National Strategy that "companies whose products or services directly or indirectly impact the economy or the health, welfare and/or safety of the public should be encouraged to purchase specific cyber risk insurance programs from financially strong insurers."

The market for cyber insurance is gaining appreciable traction. According to GartnerGroup, the Stamford Connecticut based advisory, the cyber insurance and reinsurance market is expected to grow to some $2.5 billion within the next few years, with some 25 percent of all large corporations purchasing this kind of insurance.

American International Group (AIG),[10] the leading global carrier of cyber insurance, has seen keen interest and growing uptake of cyber insurance since introducing it to the market three years ago. AIG eBusiness Risk Solutions (eBRS) and its technology partners help individuals and companies to identify, assess, mitigate, and manage cyber risk and to recover from cyber crimes and covered security breaches.

Individuals and small businesses should adopt cyber insurance as a financial risk management and risk transfer tool, enabling them to withstand attacks that circumvent the security measures they may have in place.

For example, home users wishing to protect their online exposures should purchase cyber insurance to guard against the growing incidence and costs of online identity theft since, according to government and industry estimates, individuals spend more than 175 hours of time

[9] 2002 CSI/FBI Computer Crime and Security Trends and Issues Survey, page 19.

[10] Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions. Coverage may not be available in all states. Issuance of coverage is subject to underwriting. Non-insurance products may be provided through independent third parties.

and thousands of dollars in unraveling the consequences of identity theft.[11] Insurance provides individuals with reimbursement of certain losses arising from identity theft, payment of lost wages for time spent away from work to rectify credit records, and payment of legal fees to defend suits or remove civil judgments brought as a result of identity theft. The policy can also provide personal coverage against computer viruses, cash value for computer or operating system damage, or repair costs to an individual's PC. Given that most cyber criminals perpetrate identity theft to commit other crimes, like damaging or stealing data, this component of coverage is particularly valuable. Individuals can obtain coverage directly, or through the employee payroll deduction plans of a company that's purchased coverage on behalf of its employees.

Businesses should also adopt network security insurance, since they are even more susceptible to cyber crime. For example, many small businesses are migrating to high-speed DSL or cable modem connections without adequate financial resources to deploy the necessary firewalls and other networking safeguards. Unlike regular dial-up Internet connections, "always on" connections generally assign static IP addresses, making business users sitting ducks for cyber attackers who constantly probe the Web for online vulnerabilities they can exploit. Fortunately, carriers are making available to companies of all sizes and industries cyber risk insurance policies to assist companies in their security assessment and financial risk management.

Large enterprises must take comprehensive steps to secure their networking infrastructures and manage their financial risk. The burden to do so is proportionately compounded to the extent that their networks connect multiple business partners, vendors, and customers. Thus, large corporations, especially in the financial, health care, technology, and retail sectors, are increasingly adopting cyber insurance as a component of their enterprise risk management strategies. Companies are also being held to more stringent regulatory mandates such as HIPPA (Health Insurance Portability and Accountability Act) and GLBA (Gramm-Leach-Bliley Act),

[11] United States General Accounting Office (GAO) Report to Congressional Requester, "Identity Theft: Prevalence and Cost Appear to Be Growing," GAO-02-363, March 2002. See also "The Risk to Homeland Security from Identity Fraud and Identity Theft," Testimony for the joint hearing of the House Judiciary Subcommittees on Immigration, Border Security and Claims & Crime, Terrorism and Homeland Security, June 25, 2002.

to ensure that they have taken the necessary measures to manage their information security risk.

Carriers such as AIG have expertise in information security risk management and insuring eBusiness risk, a global presence appropriate for companies with distributed networks, and adequate financial wherewithal to cover potentially catastrophic cyber events. AIG provides express cyber terrorism coverage through an endorsement of its netAdvantage® policy, which covers a range of first and third-party risks, including eBusiness interruption, loss or damage of information, and network security liability.

Businesses should make cyber terrorism and financial risk management Board-level issues, to raise awareness and build the top-down support necessary to deploy an effective enterprise-wide risk management program. "Ultimately, addressing cyber security within an enterprise is more than a technical problem, it is a management challenge," notes the National Strategy. "The scope of the risks presented by cyber security can be effectively managed by engaging senior leadership and by involving the corporate board of directors."[12]

Comprehensive Risk Management Program Strengthens Offensive Line

A complete security risk management program incorporates preventive, management and recovery measures–integrating a mix of technology, practices/procedures, and financial risk management tools, such as cyber insurance.

However, cyber insurance does more than simply defend national interests by providing financial relief for the beneficiaries of coverage in the event of a successful cyber attack. It helps fortify the offensive line against online invaders intent on doing harm. Carriers help educate government agencies, businesses, and the public about the growing perils online and recommended risk management best practices. Insurance also creates a funding mechanism, spreading financial risk so that the individual impact of an attack can be broadly absorbed without resulting in otherwise more devastating impact of a cyber disaster. Moreover,

[12] The PCIPD, *The National Strategy*, September 2002, page 19.

cyber insurance creates incentives for individuals and businesses to remain vigilant and to deploy the most effective security solutions within their means, since carriers like AIG offer premium discounts to insureds who proactively address their network vulnerabilities.

The Internet: A Shared Utility that Brings Shared Responsibility

Without insurance, a successful attack on an individual, small business, or large enterprise can have a potentially crippling ripple effect. For example, if a business network is disabled, and the company suffers shareholder lawsuits, the damage caused by the attack can have more far-reaching consequences, affecting employees and business partners as well. Thus, financial risk management benefits individuals and businesses, but its benefits roll up to the public at large as an essential means of thwarting enemy attempts to disable our Nation's critical infrastructure.

The government is doing its part by increasing security among its own agencies and by raising awareness within the private and public sectors to the shared responsibility of protecting the Nation's cyber borders. In addition, the Federal government recognized the importance of this insurance coverage by explicitly covering cyber terrorism and e-business interruption under the U.S. Terrorism Risk Insurance Act of 2002, a three-year program that ensures Federal assistance as a backstop to the private insurance industry. Individuals and businesses must do their part as well, taking every measure to more effectively manage risk and every means available to fortify the Nation's critical infrastructure. For in the end, there can be no winning the War on Terror without winning the battle online.


Prudens
Futuri